What Is Claimed Is:

1. A method of enhancing data security, which data is to be executed in an electronic device (101) comprising a secure execution environment (104) to which access is restricted, the method comprising the steps of:

generating (S303), in said secure execution environment, a new secret key repeatedly;

verifying (S302), in said secure execution environment, the integrity of data to be written into storage (110);

encrypting (S304), in said secure execution environment, the data by means of said new secret key; and

writing (S305) the encrypted data into storage.

2. The method according to claim 1, wherein a new secret key is generated when the device is booted.

3. The method according to claim 1, wherein a new secret key is generated repeatedly during runtime.

4. The method according to claim 1, wherein said data comprises program code.

5. The method according to claim 1, wherein said storage (110) comprises temporary memory.

6. The method according to claim 1, further comprising the step of:

reordering address locations of said storage (110) in address space at the time of boot, wherein the order of the address locations in address space is altered.

7. The method according to claim 4, further comprising the step of:

authenticating (S403), in said secure execution environment (104), the program code to be written into storage

(110) to ensure that the program code originates from a trusted program code provider.

8. The method according to claim 1, wherein the step of encrypting (S304) data further comprises the steps of:

combining the address of the location in said storage (110), to which location the encrypted data is to be written, with the new secret key; and

using the combination of the address and the new secret key to encrypt said data, wherein the encrypted data becomes associated with said address.

9. The method according to claim 1, wherein the step of generating (S303) a new secret key comprises the step of generating a plurality of new secret keys, wherein each new secret key is used to encrypt a respective subset of the data.

10. The method according to claim 1, further comprising the step of:

calculating (S505), in said secure execution environment (104), integrity data for data to be stored in said storage (110); and

storing (S506) the calculated integrity data.

11. The method according to claim 10, wherein said integrity data comprises a message authentication code.

12. The method according to claim 11, wherein said message authentication code is calculated by using the generated new secret key.

13. The method according to claim 12, wherein different message authentication codes are calculated for different parts of the data by means of different new secret keys.

14. The method according to claim 13, further comprising the steps of:

verifying (S602), in said secure execution environment (104), correctness of the message authentication code that is associated with read data; and

stopping (S603) device operation if said message authentication code is incorrect.

15. The method according to claim 1, further comprising the steps of:

setting a processor (103) arranged in the electronic device (101) in one of at least two different operating modes; and

storing protected data relating to device security in at least one storage area of a storage circuitry (105, 106, 107); wherein

the processor is given access to said storage area, in which said protected data are located, when a secure processor operating mode is set, and

the processor is denied access to said storage area when a normal processor operating mode is set.

16. The method according to claim 15, wherein the setting of processor modes is performed by protected applications.

17. A system for enhancing data security, which data is to be executed in an electronic device (101) comprising a secure execution environment (104) to which access is restricted, which system comprises:

means (103) arranged to generate, in said secure execution environment, a new secret key in said secure execution environment repeatedly;

means (103) arranged to verify, in said secure execution environment, the integrity of data to be written into storage (110);

means (103) arranged to encrypt, in said secure execution environment, the data by means of said new secret key; and

means (103) arranged to write the encrypted program code into storage.

18. The system according to claim 17, wherein the system is arranged such that a new secret key is generated when the device is booted.

19. The system according to claim 17, wherein the system is arranged such that a new secret key is generated repeatedly during runtime.

20. The system according to claim 17, wherein said data comprises program code.

21. The system according to claim 17, wherein said storage (110) comprises temporary memory.

22. The system according to claim 17, further comprising:

means (103) arranged to reorder address locations of said storage (110) in address space at the time of boot, wherein the order of the address locations in address space is altered.

23. The system according to claim 20, further comprising:

means (103) arranged to authenticate, in said secure execution environment (104), the program code to be written into storage (110) to ensure that the program code originates from a trusted program code provider.

24. The system according to claim 17, wherein the means (103) arranged to encrypting data further is arranged to

combine the address of the location in said storage (110), to which location the encrypted data is to be written, with the new secret key, and to use the combination of the address and the new secret key to encrypt said data, wherein the encrypted data becomes associated with said address.

25. The system according to claim 17, further comprising:

means (103) arranged to calculate, in said secure execution environment (104), integrity data for data to be stored in said storage (110); and

means (110, 112) arranged to store the calculated integrity data.

26. The system according to claim 25, wherein said integrity data comprises a message authentication code.

27. The system according to claim 26, wherein the calculating means (103) is arranged such that it uses the new secret key generated to calculate the message authentication code.

28. The system according to claim 27, further comprising:

means (103) arranged to verify, in said secure execution environment (104), correctness of the message authentication code that is associated with read data and to stop device operation if said message authentication code is incorrect.

29. The system according to claim 17, further comprising:

a processor (103) arranged such that it may be set in one of at least two different operating modes; and

storage circuitry (105, 106, 107) arranged with at least one storage area in which protected data relating to

device security are located; wherein the system is further arranged such that:

the processor is given access to said storage area, in which said protected data are located, when a secure processor operating mode is set, and

the processor is denied access to said storage area when a normal processor operating mode is set.

30. The system according to claim 29, wherein the setting of processor (103) modes is performed by protected applications.

31. A mobile telecommunication terminal (100, 200) comprising the system according to claim 17.

32. A programmable logic device (101, 201) comprising the system according to claim 17.

33. The programmable logic device (101, 201) according to claim 32, wherein said programmable logic device is implemented in the form of an application specific integrated circuit.

34. A computer program comprising computer-executable components for causing a device (101) to perform the steps recited in claim 1 when the computer-executable components are run on a processing unit (103, 203) included in the device.

35. A computer-readable medium storing computer-executable components for causing a device (101) to perform the steps recited in claim 1 when the computer-executable components are run on a processing unit (103, 203) included in the device.